COLORADO
Information Security
Governor's Office of Information Technology

Secure Colorado

Colorado's Strategy for Information Security and Risk Management

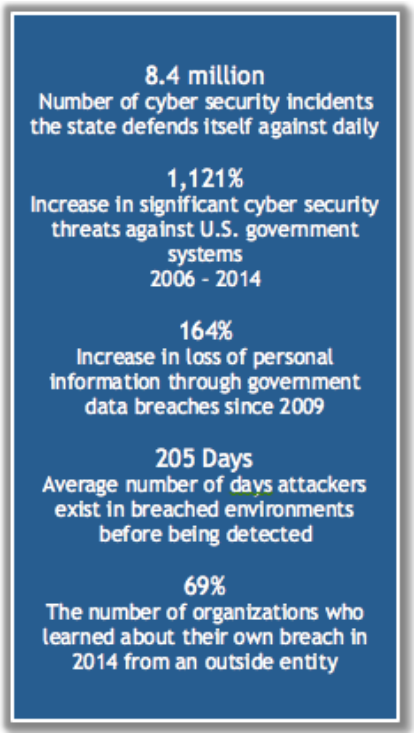
Fiscal Years 2016-2018

Table of Contents

SECTION I - INTRODUCTION AND BACKGROUND

CONTINUING THE JOURNEY

In 2012, Chief Information Security Officer (CISO) Jonathan Trull, with the help of the 2012 Colorado Information Security Advisory Board, created our state's first cyber security strategic plan. The plan was a call to action, acknowledging the criticality of state information assets, the need to protect those assets, and the fact that the state was continually under cyber attack, defending against 600,000 security incidents daily.



The threat has escalated. While tools have given us better visibility into security incidents, the attack volume has also increased significantly. We are currently defending our state network against ***8.4 million security incidents per day***. The volume and sophistication of attacks continues to increase, and every indication is that the number of attacks will continue to rise for the foreseeable future.

This strategic plan, known as **Secure Colorado**, set the stage for ongoing security improvements, creating a budget and enabling strategic decisions and investments to protect the data Coloradans have entrusted to state government. **Secure Colorado** outlines the strategic goals and initiatives of the Colorado Information Security Program to safeguard the state's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve the State of Colorado's mission.

While the inaugural version of Secure Colorado was meant to conclude at the end of fiscal year 2016, we all know that security is never "done". Technological advancements, the increasing sophistication of attacks, and evolving business needs, mean that we need to continue to reassess and evolve our security strategy.

In 2015, the Colorado Information Security Advisory Board reconvened to receive an update on our progress and to reevaluate Secure Colorado. The Board overwhelmingly found the direction and program priorities relevant, appropriate, and sound. With the Board's recommendation, we are adopting Secure Colorado as our ongoing multi-year strategic roadmap, and broadening it to encompass fiscal year 2016-2018 and future needs. Updating this multi-year strategy annually, will ensure we maintain momentum and focus, continuing to improve our cyber security program for the benefit of the agencies we serve and all Colorado residents.

Sincerely,

Deborah M. Blyth, Chief Information Security Officer

INFORMATION SECURITY GOVERNANCE

The Colorado Information Security Program was created through legislation in 2006. According to Colorado law (C.R.S. § 24 -37.5-4xx), the Colorado Information Security Program is overseen by the Chief Information Security Officer (CISO) and applies to "public agencies." A public agency is defined as: …every state office, whether executive or judicial, and all its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

According to statute, the CISO shall:

- Develop and update information security policies, standards, and guidelines for public agencies.
- Promulgate rules containing information security policies, standards, and guidelines.
- Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies.
- Direct and respond to information security audits and assessments in public agencies in order to ensure program compliance and adjustments.
- Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.
- Approve or disapprove and review annually the information security plans of public agencies.
- Conduct information security awareness and training programs.
- In coordination and consultation with the Office of State Planning and Budgeting and the Chief Information Officer (CIO), review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the legislative branch.
- Coordinate with the Colorado Commission on Higher Education for purposes of reviewing and commenting on information security plans adopted by Institutions of Higher Education.
- Oversee incident response activities as well as the investigation of security breaches, and assist with the disciplinary and legal matters associated with such breaches as necessary and maintain authority to direct discontinuation of services from unsafe systems.
- Maintain relationships with local, state and federal partners and other related private and government agencies.

Within the Governor's Office of Information Technology (OIT), the CISO reports to the CIO. Information security duties and responsibilities for executive branch agencies are administratively divided between the CISO and the Chief Technology Officer (CTO). While the CISO maintains responsibility for information security governance, architecture, risk, and compliance, the CTO is responsible for overseeing day-to-day security operations, including access provisioning, network and endpoint security monitoring and administration, threat and vulnerability management, and computer forensics and incident response.

OIT MISSION AND GOALS

It is important that **Secure Colorado** aligns with OIT's mission and goals, which in turn are aligned with the Governor's strategic plan. Protecting citizen data is required to align to OIT's mission.

Mission:
To securely enable the effective, efficient and elegant delivery of government services through trusted partnerships and technology.

Our passion, purpose, and motivation is to serve the state of Colorado. We collaborate with customers to provide day-to-day digital support and present smart solutions that transform government through IT. We push ourselves to deliver next generation, integrated technology in order to create a dynamic end-user experience for Coloradans and offer the expertise our customers expect.

Goals:
OIT has four strategic goals (also known as Wildly Important Goals) which are intended to focus on service excellence, ***information security***, employee engagement, and IT job growth across Colorado.

In early 2015, Colorado was recognized by the Brookings Institution as being one of only two states demonstrating a "solid and robust" understanding of the importance of integrating cyber security in their strategic IT plans *http://statescoop.com/idaho-mississippi-lead-states-cybersecurity-plans-report*

COLORADO INFORMATION SECURITY PROGRAM VISION AND MISSION

The following are the vision and mission for the Colorado Information Security Program, including a description of our philosophy for tackling the state's information security challenges and assuring the confidentiality, integrity, and availability of state networks, systems, and data.

Vision

Cost-effectively preserving the confidentiality, integrity, and availability of state and citizen data through the innovative use of the right people, processes, and technology.

Mission

Enable the State of Colorado to achieve its business objectives by maintaining an appropriate level of information security risk that promotes innovation, the effective use and adoption of information and information technologies, and fosters citizen engagement and e-commerce.

Team Slogan

Together, enabling state government operations through the efficient, effective, and elegant application of information security.

Philosophy Toward Information Security and Risk Management

Our philosophy describes how we approach the development of solutions for securing Colorado's information and systems. The Colorado Information Security Program will perform its work according to the following principles:

1. Offense must inform defense
2. Security must be built into business processes and IT systems from the start
3. Cyber threats are mitigated through the right combination of people, processes, and technology
4. Our security efforts must first be focused on our high value targets
5. Complexity is the enemy of security
6. Automated controls are superior to manual controls
7. Security drives compliance and not vice versa
8. Security must be efficient - only those security resources necessary to achieve our mission are acquired and deployed
9. Security must be effective - security must be results-oriented and anticipated outcomes measured, tracked, and compared to the resources expended
10. Security must be elegant – the most effective controls and security solutions are those that are transparent to the business and end user and seamlessly integrate with the state's business processes and existing technology

SECTION II - STRATEGIC PRIORITIES

Secure Colorado establishes a roadmap for improving cyber security in Colorado over the next three years. This plan was developed in cooperation with the Colorado Information Security Advisory Board (Board). The Board was formed by the CISO in 2012 to assist in the development of strategic and tactical plans aimed at reducing the State of Colorado's risk levels and improving the confidentiality, integrity, and availability of the information entrusted to the state. The Board met again in 2015, with almost half of the original members returning, and were joined by some new members. These individuals represent public and private sectors, along with higher education, and include security, privacy, and business professionals. See Appendix A for 2015 Board Membership.

Secure Colorado includes four strategic goals supported by 18 strategic initiatives. These goals and initiatives are based on foundational information security principles that are designed to be relevant for years to come. Supporting operational initiatives will be developed annually and included in the OIT Playbook, which can be found on the OIT's website – www.colorado.gov/oit. These operational-level initiatives will be the Colorado Information Security Program's primary focus for that specific fiscal year and will be aligned with one or more of Secure Colorado's strategic goals and initiatives.

To maintain its relevancy, Secure Colorado will be reviewed annually by the CISO, in conjunction with the Colorado Information Security Advisory Board and OIT Executive Leadership Team.

PROTECTION

Goal # 1 - Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats

STRATEGIC INITIATIVES

Initiative # 1.1 - Design, build, and operate resilient and self-healing systems and networks that are capable of resisting current and emerging cyber security threats.

Initiative # 1.2 – Recruit, develop, and retain a motivated, professional, and knowledgeable information security workforce.

Initiative # 1.3 - Design, build, and operate the necessary tools, techniques, and procedures to maintain "24/7" information security situational awareness of all state networks, systems, and data.

Initiative # 1.4 - Develop and maintain information security policies, standards, and guidelines that are relevant, adaptable, and cost-effective.

Initiative # 1.5 - Promote the understanding and acceptance of information security concepts and practices throughout state government.

Initiative # 1.6 - Equip state information technology professionals with the tools, knowledge, and skills to design, build, and operate secure applications and systems.

Initiative # 1.7 – Develop, document, and socialize an information security architecture that (1) aligns with the technology strategy, (2) transparently integrates security processes into next-generation state networks and systems, and (3) anticipates and addresses future threats.

Initiative # 1.8 – Develop and maintain a statewide incident response and computer forensic capability that is able to (1) quickly identify and isolate security incidents, (2) recover impacted systems and business processes, and (3) when feasible, identify and prosecute those attacking state systems.

Initiative # 1.9 – Develop, document, and implement a standardized risk management framework for accurately and uniformly assessing and managing the risk to the confidentiality, integrity, and availability of state systems and networks.

RESEARCH AND DEVELOPMENT

Goal # 2 - Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cyber security challenges

STRATEGIC INITIATIVES

Initiative # 2.1 - Actively leverage federal government, private sector, academic research, and development of advanced cyber security tools and capabilities to assure the confidentiality, integrity, and availability of state systems and data.

Initiative # 2.2 - Rapidly evaluate, build, and deploy cutting-edge information security technologies to outpace emerging threats.

Initiative # 2.3 – Identify, evaluate, and share information on the threats and vulnerabilities impacting state government to support future research and development efforts.

PARTNERSHIPS

Goal # 3 - Develop and foster key partnerships to improve information sharing, reduce information security risks, and to promote innovation and collaboration

STRATEGIC INITIATIVES

Initiative # 3.1 - Develop and formalize new partnerships with academic institutions, the private sector, and Colorado's state and local governments to share information security threat intelligence, research and development efforts, and best practices.

Initiative # 3.2 – Maintain active participation with the relevant organizations such as the National Association of State Chief Information Officers' (NASCIO) Privacy and Security Committee, Multi-State Information Sharing Analysis Center (MS-ISAC), and the SANS Institute.

Initiative # 3.3 – Promote discussions and cooperative engagements that will enhance cyber security for all Colorado residents including partnering with the Colorado Department of Public Safety in achieving the cyber security objectives of the Colorado Division of Homeland Security and Emergency Management strategy.

COMPLIANCE

Goal # 4 - Comply with applicable information security and data privacy laws and regulations

STRATEGIC INITIATIVES

Initiative # 4.1 - Continuously assess and evaluate state systems and networks.

Initiative # 4.2 – Conduct targeted, technical audits to identify and correct non-compliance with state Information Security Policies and applicable federal laws and regulations.

Initiative # 4.3 – Partner with executive branch agencies to assist them in preparing for and responding to information security-related audits.

SECTION III - STRATEGIC SUCCESS MEASURES

Metric Name	Target	Reporting Frequency	Description
Goal # 1 - Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats			
Percentage of State Systems Actively Managed by Security	100%	Monthly	Percentage of total state systems actively managed and protected (in near real-time).
Composite Information Security Risk Index	LOW	Quarterly	Overall, enterprise-level cyber security risk rating based on current threats, asset value, and implemented security controls.
Mean Time from Incident Detection to Containment and Restoration	< 4 hours	Quarterly	Measures the average length of time necessary to contain a security incident and restore impacted services.
Percentage of Employees Completing Security Training	95%	Monthly	Percentage of state employees completing security training, including new employee training, refresher training, and technical security training.
Goal # 2 - Research, develop, and employ innovative and sustainable information security solutions to address Colorado cyber security challenges			
Percentage of State IT Expenditures Spent on Information Security	5%	Annual	Measures the percentage of IT expenditures utilized to design, build, and implement innovative and sustainable information security solutions.
Number of Emerging Cyber Security Product Evaluations Completed	3	Annual	Represents the number of emerging security product reviews completed annually to address emerging cyber security challenges.
Mean Time from Product Evaluation and Selection to Deployment	< 120 days	Annual	The average number of days elapsed between the completion of an emerging cyber security need to a recommended solution.

Goal # 3 - Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration			
Number of Active Information Sharing Agreements	Tracking Only	Annual	Tracks the number of partners for which the security program shares threat and vulnerability information.
Number of Security Thought Papers / Evaluation Products Shared with Partners	>4	Annual	Number of written cyber security product evaluations and “thought” papers shared with partners.
Goal # 4 - Comply with applicable information security and data privacy laws and regulations			
Number of Managed Security Audit Findings	Tracking Only	Quarterly	Tracks the total number of security-related audit findings actively being managed by the security team.
Percentage of Overdue Security Audit Findings	10%	Quarterly	Percentage of security-related audit findings that are not implemented and are past their agreed-to implementation date.
Average Number of New Security Audit Findings Per External Audit/ Inspection	< 8	Annual	The average number of new security-related audit findings per external party audit.

APPENDIX A - COLORADO INFORMATION SECURITY ADVISORY BOARD

2015 Colorado Information Security Advisory Board	
Alfritch Anderson Security Operations Manager Governor's Office of Information Technology	**Col. Gregory A. Miller** Deputy Chief of Staff Colorado Army National Guard
Dr. Beth Bean Chief Research Officer Department of Higher Education	**Ted Mink** Deputy Director Colorado Bureau of Investigation
Eric Bergman Policy and Research Supervisor Colorado Counties, Inc.	**Robert Ochoa** Account Manager Security Cisco
Casey Carlson Enterprise Architect Governor's Office of Information Technology	**Alan Paller** Founder and Director of Research SANS Institute
Rick Dakin Co-Founder and CEO Coalfire Systems	**Chris Payne** Sr. Security Engineer McAfee
Andrea Day OSPB Analyst Governor's Office of State Planning and Budgeting	**Robert Rudloff** Partner Rubin Brown Cyber Security Practice
Nicole Frazier Denver Metro Regional Director Office of Senator Cory Gardner	**Fred Sargeson** General Manager Colorado Interactive
Ralph Gagliardi Agent-in-Charge, Identity Theft Advocacy Network Colorado Bureau of Investigation	**Sam Searcy** CEO, Data Communications Management, Inc., and Board of Directors Space Age Federal Credit Union
Don Wisdom Director, Infrastructure Operations Governor's Office of Information Technology	**Rich Schliep** CISO Colorado Secretary of State's Office
Tim Gama Program Coordinator Pueblo Community College	**Ron Sloan** Director Colorado Bureau of Investigation
Kent Glassman Glassman and Associates	**Lyn Snow** Chief Privacy Officer Colorado Department of Human Services

Dan Jones Assistant Vice President and CISO University of Colorado System	**David Spector** Senior Deputy Legal Counsel Office of the Governor
Dan Krug Financial Planning & Ops Director Governor's Office of Information Technology	**Trevor Timmons** CIO Colorado Secretary of State's Office
Amelia Larsen Program Manager Health Information Office Department of Health Care Policy & Financing	**Paul Underwood** Managing Partner and COO Emagined Security
Mark Lewis Manager,Western Region Engineers McAfee	**Steve White** Director, Security & Compliance CenturyLink
Jory Maes CO Infrastructure Protection Program Manager Colorado Department of Public Safety, Division of Homeland Security & Emergency Management	**Jane Wilson** Privacy Officer Department of Health Care Policy and Financing
Chetna Mahajan Director of Enterprise Applications Governor's Office of Information Technology	**Michael Wyatt** Director Public Sector Cyber Risk Services Deloitte
LTC Isaac Martinez Deputy Chief of Staff Colorado Army National Guard	